UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/539,164	06/15/2005	Yoshihiko Takagi	38355	2649

52054 7590 09/24/2008

PEARNE & GORDON LLP
1801 EAST 9TH STREET
SUITE 1200
CLEVELAND, OH 44114-3108

EXAMINER	
SHEPELEV, KONSTANTIN	
ART UNIT	PAPER NUMBER
2131	

NOTIFICATION DATE	DELIVERY MODE
09/24/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patdocket@pearne.com
dchervenak@pearne.com

Office Action Summary	Application No.	Applicant(s)	
	10/539,164	TAKAGI ET AL.	
	Examiner	Art Unit	
	KONSTANTIN SHEPELEV	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 June 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/15/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to application filed on June 15, 2005 in which claims 1-16 are presented for examination.

Status of Claims

Claims 1-16 are pending; of which claims 1 and 12 are in independent form. Claims 1, 2, 5, and 16 are rejected under 35 U.S.C. 102(b). Claims 3, 4, 6-11 and 12-15 are rejected under 35 U.S.C. 103(a).

Specification

1. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: Semiconductor memory card utilizing secure non-tamper resistant memory accessed only through secure control unit.

Claim Objections

2. Claims 13 and 15 objected to because of the following informalities: Claim 13 recites "the electronic device according to claim 13" which appears to be a misprint. Examiner interpreted the claim to be dependent upon claim 12. Furthermore, claim 15 recites "the electronic device according to claim 15" which also appears to be a misprint. Examiner interpreted this claim as being dependent upon claim 12. Appropriate corrections are required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1, 2, 5, and 16 are rejected under 35 U.S.C. 102(b) as being anticipated by Schwartz (US 4,985,921).

With respect to claim 1, Schwartz discloses the limitation of "first memory of non-tamper-resistance having a usual area that can be accessed from the electronic device and a secure area that cannot directly be accessed from the electronic device" (Fig. 1; column 2, lines 42-46) as the control unit 2 preferably comprises a microprocessor with a computer and RAM and ROM storage areas as well as additionally a data memory region, where (column 3, lines 3-5) the data exchange within the component 2 between the control unit and data memory existing there is produced in a similarly protected manner.

In addition, Schwartz discloses the limitation of "second memory of tamper resistance that cannot directly be accessed from the electronic device" (Fig. 1; column 2, lines 45-46) as an additional data memory exists on the second component, where (column 2, lines 62-64) in order to prevent manipulation and unauthorized access to the data memory 5, entry to this memory is protected by the control unit.

Finally, Schwartz discloses the limitation of "a secure control section for controlling access to the second memory, wherein access to the secure area of the first memory from the electronic device can be made only through the secure control section" (column 2, lines 62-64) in

order to prevent manipulation and unauthorized access to the data memory 5, entry to this memory is protected by the control unit. The data exchange within the component 2 between the control unit and data memory existing there is produced in a similarly protected manner (column 3, lines 3-5).

With respect to claim 2, Schwartz discloses the limitation of "upon reception of a command from the electronic device authenticated by the secure control section, the secure control section accesses the secure area or the second memory and writes or reads data" (column 2, line 66 – column 3, line) as the memory is accessible only by means of a code signal C which is produced by the control unit, that is, data exchange between the components is only possible after successful decoding of the code region.

With respect to claim 5, Schwartz discloses the limitation of "the usual area of the first memory includes an authentication area that can be accessed only by electronic devices authenticated by a general control section for controlling the memory device and a non-authentication area that can be accessed even by an electronic device not authenticated" (column 2, lines 53-58) as an external connection to the control unit can only be made by means of the contact 9 so that an exchange of sensitive data between the card and the system in a known fashion can only come about after successful authentication and identification, which functions are participated in by the control unit.

With respect to claim 16, Schwartz teaches the limitation of "the memory device is connected to an electronic device fixedly or detachably" (Abstract) as a portable data carrying device intended for the required connection by means of contacts to an external read/write unit.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schwartz (US 4,985,921) in view of Ferreira (US 6,115,601).

With respect to claim 3, Schwartz teaches the limitation of "an encryption key is stored in the second memory" (column 3, lines 11-14) as the access to the sensitive data in the data memory 5 is protected by means of a barrier which can only be overcome by means of a key codes employed within the card.

It is noted, however, that Schwartz does not explicitly teach the limitation of "the secure control section encrypts the data to be written into the secure area using the encryption key and writes the encrypted data and decrypts the data read from the secure area using the encryption key."

On the other hand, Ferreira teaches the abovementioned limitation (column 6, lines 54-59) as the secure module also comprises authenticator for authenticating messages. Optionally,

the authenticator may also be used for securing some of the data stored in the memory of the secure module, for instance by suitably encrypting/decrypting the data.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Ferreira into the system of Schwartz to further secure data stored in the memory.

With respect to claim 4, it is noted that Schwartz does not explicitly teach the limitation of "the secure control section calculates a hash value of the data to be written into the secure area, stores the hash value in the second memory, calculates a hash value of the data read from the secure area, and compares the hash value with the hash value stored in the second memory."

On the other hand, Ferreira teaches the abovementioned limitation (column 7, line 67 – column 8, line 6) as a message authentication code is generated by a key-dependent one-way hash function. The receiving party uses the same key-dependent one-way hash function to hash the plaintext elements and checks whether the resulting hash value matches the received Message Authentication Code.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Ferreira into the system of Schwartz to provide an authentication method which preferably also reduces the size of the data.

7. Claims 6-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schwartz (US 4,985,921) in view of Hirota et al (EP 1,050,887 A1).

With respect to claims 6-11, Schwartz teaches a portable memory device with public and secure memories, where access to the memory areas is controlled by a processor.

It is noted, however, that Schwartz does not explicitly teach the controller adjustable boundary between the secure and common areas of the memory represented by the address information in the address translation tables.

On the other hand, Hirota teaches the limitations of claims 6-11 in the following way:

With respect to claim 6, Hirota teaches the limitation of "boundary address information indicating the boundary between the usual area and the secure area and logical-physical address translation tables describing the relationship between logical addresses and physical addresses in the usual area and the secure area are managed as address information of the first memory" (column 4, paragraph 0020) as the area resizing circuit resizes the authentication area and the non-authentication area by changing an address making a boundary between the authentication area and non-authentication area.

With respect to claim 7, Hirota teaches the limitation of "the usual area of the first memory includes an authentication area that can be accessed only by electronic devices authenticated by a general control section for controlling the memory device and a non-authentication area that can be accessed even by an electronic device not authenticated" (column 2, paragraph 0008) as a rewritable non-volatile memory and a control circuit which controls accesses by the electronic device to an authentication area and a non-authentication area in the rewritable non-volatile memory.

In addition, Hirota teaches the limitation of "the address information of the first memory includes boundary address information indicating the boundary between the authentication area and the non-authentication area and logical-physical address translation tables in the authentication area and the non-authentication area" (column 4, paragraph 0022) as an authentication area conversion table, a non-authentication conversion table, and (column 4, paragraph 0020) an address marking a boundary between the authentication area and the non-authentication area.

With respect to claim 8, Hirota teaches the limitation of "the boundary address information and the logical-physical address translation tables are recorded in an address information management area of the first memory" (column 3, paragraph 0018) as an area resizing circuit of the semiconductor memory card, which contains (column 4, paragraph 0022) an authentication area conversion table, a non-authentication conversion table, and (column 4, paragraph 0020) an address marking a boundary between the authentication area and the non-authentication area.

With respect to claim 9, Hirota teaches the limitation of "the boundary between the usual area and the secure area represented by the boundary address information is changed according to a command of the electronic device authenticated by the secure control section" (column 4, paragraph 0022) as a conversion table change unit changes contents of the authentication area conversion table and the non-authentication table conversion table in accordance with an instruction from the electronic device.

With respect to claim 10, it is rejected in view of the same reasons stated in the rejection of claim 9.

With respect to claim 11, Hirota teaches the limitation of "wherein the boundary address information of the boundary between the authentication area and the non-authentication area is made up of a real boundary address and an assumed boundary address set with the secure area excluded" and "the real boundary address is changed based on the assumed boundary address specified by a command of the electronic device authenticated by the general control section" (column 4, paragraph 0024) as an area addressed with higher physical addresses and an area addressed with lower physical addresses both constituting the area having the predetermined size may be respectively allocated to the authentication area and the non-authentication area, the non-authentication area conversion table shows correspondence between logical addresses arranged in ascending order and physical addresses arranged in the ascending order and the authentication area conversion table shows correspondence between logical addresses arranged in the ascending order and physical addresses arranged in descending order.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Hirota into the system of Schwartz to provide a flexible secure method for memory management of the data memory region because it would provide a better security for the stored data.

8. Claim 12-15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hirota et al (EP 1,050,887 A1) in view of Schwartz (US 4,985,921).

With respect to claim 12, Hirota teaches the limitations of "the electronic device accesses the first area of a non-tamper-resistant memory area of the memory device through a general control section of the memory device for controlling access to the memory device", "after authenticated by the general control section and a secure control section of the memory device for controlling access to the second area and the third area, accesses the second area of a non-tamper-resistant memory area through the secure control section", and "after authentication with the secure control section, accesses the third area of a tamper-resistant memory area of the memory device through the general control section and the secure control section" (column 2, paragraph 0008) as a semiconductor memory card that can be used in an electronic device, comprising a rewritable non-volatile memory, and a control circuit which controls accesses by the electronic device to an authentication area and a non-authentication area in the writable non-volatile memory. The control circuit includes a non-authentication area access control unit which controls accesses by the electronic device to the non-authentication area, an authentication unit which performs an authentication process to check whether the electronic device is proper, and affirmatively authenticates the electronic device when the electronic device is proper, and authentication access control unit which permits the electronic device to access the authentication area only when the authentication unit affirmatively authenticates the electronic device.

It is noted that Hirota does not explicitly teach the distinction between tamper resistant memory and non-temper resistant memory.

On the other hand, Schwartz teaches (column 2, lines 42-46) the control unit preferably comprises a microprocessor with a computer and RAM and ROM storage areas as well as a data memory region. An additional data memory exists on the second component.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to combine teachings of Schwartz with teachings of Hirota because such combination would provide safer storage environment for the electronic data.

With respect to claim 13, Hirota teaches the limitation of "first command generator which generates a command for writing or reading data into or from the first area" (Fig. 5) as Non-Authentication Area Access control unit 326.

In addition, Hirota teaches the limitation of "second command generator which generates a command for requesting the secure control section to perform processing" (Fig. 5) as Special Area Access control unit 324.

Finally, Hirota teaches the limitation of "first authentication processor which acquires an authentication key used for authentication with the secure control section and perforating performs authentication processing with the secure control section" (Fig. 5) as Authentication Unit 321.

With respect to claim 14, Hirota teaches the limitation of "a non-authentication area of a partial area of the first area is accessed without authentication with the general control section and an authentication area of a part or all of the first area other than the non-authentication area is accessed after authentication with the general control section" (column 2, paragraph 0008) as

the control circuit includes a non-authentication area access control unit which controls accesses by the electronic device to the non-authentication area, an authentication unit which performs an authentication process to check whether the electronic device is proper, and affirmatively authenticates the electronic device when the electronic device is proper, and authentication access control unit which permits the electronic device to access the authentication area only when the authentication unit affirmatively authenticates the electronic device.

With respect to claim 15, it is noted that Hirota does not explicitly teach the limitations of "third command generator which generates a command for writing or reading data into or from the authentication area" and "second authentication processor which acquires an authentication key used for authentication with the general control section and performs authentication processing with the general control section".

On the other hand, Schwartz teaches the abovementioned limitation of "third command generator which generates a command for writing or reading data into or from the authentication area" (Fig.2; column 2, lines 53-58) as the control unit 2a protecting data memory from an unauthorized access.

In addition, Schwartz teaches the limitation of "second authentication processor which acquires an authentication key used for authentication with the general control section and performs authentication processing with the general control section" (Fig. 2; lines 28-37) as the component 4a contains microprocessor in addition to data memory which helps to secure entry to the data memory from control unit 2.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Schwartz into the system of Hirota to secure the data exchange between the second protected memory and the main controller by providing an additional level of data exchange validation.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

a. Richter (US 6,975,883 B1).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KONSTANTIN SHEPELEV whose telephone number is (571)270-5213. The examiner can normally be reached on Mon - Thu 8:30 - 18:00, Fri 8:30 - 17:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Konstantin Shepelev/ 9/18/2008
Examiner, Art Unit 2131

/Syed Zia/
Primary Examiner, Art Unit 2131